A Family of Quantum Stabilizer Codes Based on the Weyl Commutation Relations over a Finite Field

V. Arvind and K. R. Parthasarathy
Institute of Mathematical Sciences, C.I.T Campus
Chennai 600113, India
email: {arvind,krp}@imsc.ernet.in

Dedicated to C.S. Seshadri on his 70th birthday

Abstract

Using the Weyl commutation relations over a finite field $\mathbb{F}_q$ we introduce a family of error-correcting quantum stabilizer codes based on a class of symmetric matrices over $\mathbb{F}_q$ satisfying certain natural conditions. When $q = 2$ the existence of a rich class of such symmetric matrices is demonstrated by a simple probabilistic argument depending on the Chernoff bound for i.i.d symmetric Bernoulli trials. If, in addition, these symmetric matrices are assumed to be circulant it is possible to obtain concrete examples by a computer program. The quantum codes thus obtained admit elegant encoding circuits.

1 Introduction

Let A be a finite abelian group with operation denoted by $+$ and identity 0. We identify A with the alphabet of symbols transmitted on a classical communication channel. Consider the n-fold cartesian product A^n of copies of A. Elements of A^n are called words of length n. A commonly used group is $\{0, 1\}$ with addition modulo 2. Let $\hat{A}$ denote the character group of A, the multiplicative group of all homomorphisms from A into the multiplicative group of complex numbers of modulus unity. For $\mathbf{a} = (a_1, a_2, \ldots, a_n)^T \in A^n$ we define its weight $w(\mathbf{a})$ to be $\#\{i \mid a_i \neq 0\}$. We say that a subgroup $\mathcal{C}_n$ of A^n is a *t-error correcting group code* if for every non-zero element $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ in $\mathcal{C}_n$, $w(\mathbf{x}) \geq 2t + 1$. In other words, if messages transmitted through a noisy channel are encoded into words from $\mathcal{C}_n$ and during transmission of a word errors at the output occur in at most t positions, then the message can be decoded without any error. There is a vast literature on the construction of t-error correcting group codes and the reader may find an introduction to this subject and pointers to literature in [8, 7].

A broad class of quantum error correcting codes known as stabilizer codes was introduced by Gottesman [4] and Calderbank et al [2] (also see [3, 13, 12]). To the best of our knowledge, apart from one computer-generated example [13], all quantum error-correcting codes are stabilizer codes. Our aim is to give a new description of the theory of error-correcting quantum stabilizer codes. First we introduce some definitions. We choose and fix an N-dimensional complex Hilbert space $\mathcal{H}$ and consider the unit vectors of $\mathcal{H}$ as pure states of a finite level quantum system. If A is a finite abelian group with N elements and $\{e_x \mid x \in A\}$ is an orthonormal basis of $\mathcal{H}$ indexed by elements of A we express it in the Dirac notation as $|x\rangle = e_x$. If $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in A^n$ is a word of length n, we write

$$|\mathbf{x}\rangle = |x_1 x_2 \dots x_n\rangle = e_{x_1} \otimes e_{x_2} \otimes \dots \otimes e_{x_n}$$

where the right-hand side is a product vector in the n-fold tensor product $\mathcal{H}^{\otimes^n}$ of n copies of $\mathcal{H}$. Thus, with the chosen orthonormal basis, every word $\mathbf{x}$ in A^n is translated into a basis state $|\mathbf{x}\rangle$ of $\mathcal{H}^{\otimes^n}$.

A *quantum code* is a subspace $\mathcal{C}_n$ in $\mathcal{H}^{\otimes^n}$. Note that a pure state in $\mathcal{H}^{\otimes^n}$ described by a unit vector $|\psi\rangle$ in $\mathcal{H}^{\otimes^n}$ has density matrix $|\psi\rangle\langle\psi|$. A density matrix ρ in $\mathcal{H}^{\otimes^n}$ is a non-negative operator of unit trace. In quantum probability, a projection operator E in $\mathcal{H}^{\otimes^n}$ is interpreted as an event concerning the quantum system and a density matrix ρ as a state of the quantum system. The probability of the event E in the state ρ is given by $Tr\rho E$. Messages to be transmitted through a quantum channel are encoded into pure states in $\mathcal{H}^{\otimes^n}$. When a pure state $|\psi\rangle$, or equivalently, a density matrix $|\psi\rangle\langle\psi|$ is transmitted the channel output is hypothesized to be a state of the form

$$\rho = \sum_i L_i |\psi\rangle\langle\psi| L_i^\dagger \tag{1}$$

where the operators $\{L_i\}$ belong to a linear subspace $\mathcal{A}$ of the algebra of all operators on $\mathcal{H}^{\otimes^n}$. The operators $\{L_i\}$ may depend on ρ, but in order to ensure that ρ is a density matrix it is assumed that $\langle\psi| \sum_i L_i^\dagger L_i |\psi\rangle = 1$. By the spectral theorem ρ can be expressed as

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$$

where ψ_j is an orthonormal set in $\mathcal{H}^{\otimes^n}$ and $\{p_j\}$ is a probability distribution with $p_j > 0$ for each j. In other words, the output state ρ is not necessarily pure even though the input state is pure. The operators L_i are called *error operators* and the linear space $\mathcal{A}$ from which they come is called the *error space*.

Suppose there is a finite family $\{M_j\}$ of operators in $\mathcal{H}^{\otimes^n}$ satisfying the condition $\sum_j M_j^\dagger M_j = I$ and for any output state ρ with ψ in the code $\mathcal{C}_n$,

$$\sum_j M_j \rho M_j^\dagger = \sum_{i,j} M_j L_i |\psi\rangle\langle\psi| L_i^\dagger M_j \dagger = |\psi\rangle\langle\psi|.$$

Then we say that the quantum code $\mathcal{C}_n$ together with the family $\{M_j\}$ of 'decoding operators' corrects any error induced by $\{L_i\}$ from $\mathcal{A}$. In this context we have the following fundamental theorem of Knill and Laflamme [5] which gives necessary and sufficient conditions for the existence of such a family of decoding operators.

Theorem 1.1 [5] *Let $\mathcal{A}$ be a family of operators in $\mathcal{H}^{\otimes^n}$ and let $\mathcal{C}_n \subset \mathcal{H}^{\otimes^n}$ be a quantum code with an orthonormal basis $\psi_1, \psi_2, \ldots, \psi_d$. Then there exists a finite family $\{M_j\}$ of operators in $\mathcal{H}^{\otimes^n}$ satisfying the conditions:*

(i) $\sum_j M_j^\dagger M_j = I$; *and*

(ii)

$$\sum_j M_j L|\psi\rangle\langle\psi|L^\dagger M_j^\dagger = \langle\psi|L^\dagger L|\psi\rangle|\psi\rangle\langle\psi| \quad \forall \quad \psi \in \mathcal{C}_n, L \in \mathcal{A}$$

if and only if the following condition holds:
$\langle\psi_p|L_1^\dagger L_2|\psi_q\rangle = \delta_{p,q} c(L_1, L_2)$ *for all* $L_1, L_2 \in \mathcal{A}$, $1 \le p, q \le d$, *where* $c(L_1, L_2)$ *is a scalar independent of* p *and* q *and* $\delta_{p,q}$ *is 1 if* $p = q$ *and 0 otherwise.*

Remark 1.2 *The proof of the above theorem is constructive and therefore yields the decoding operators in terms of $\mathcal{A}$ and the basis $\psi_1, \ldots, \psi_d$ of $\mathcal{C}_n$. In this case we say that $\mathcal{C}_n$ is an $\mathcal{A}$-error correcting quantum code.*

Now we specialize the choice of $\mathcal{A}$. Consider all unitary operators in $\mathcal{H}^{\otimes^n}$ of the form $U = U_1 \otimes U_2 \otimes \ldots \otimes U_n$ where each U_i is a unitary operator on $\mathcal{H}$ and all but t of the U_i's are equal to I. Such a U when operating on $\psi = \psi_1 \otimes \ldots \otimes \psi_n \in \mathcal{H}^{\otimes^n}$ produces $U|\psi\rangle$ which is an n-fold tensor product that differs from ψ in at most t places. Denote by $\mathcal{A}_t$ the linear span of all such unitary operators U. A quantum code $\mathcal{C}_n$ is called a *t-error correcting quantum code* if $\mathcal{C}_n$ is an $\mathcal{A}_t$-correcting quantum code.

2 Quantum codes and subgroups of the error group

Let $(A, +)$ be a finite abelian group with N elements and identity denoted by 0. Denote by $\hat{A}$ the character group of A and $\mathcal{H}$ the N-dimensional Hilbert space $L^2(A)$ of all complex-valued functions on A, spanned by $\{|x\rangle\}_{x\in A}$ (where the vector $|x\rangle$ denotes the indicator function 1_x of the singleton $\{x\}$). Define the unitary operators U_a and V_χ on $\mathcal{H}$ for every $a \in A$ and $\chi \in \hat{A}$ by

$$U_a|x\rangle = |x + a\rangle, \qquad V_\chi|x\rangle = \chi(x)|x\rangle$$

where $x \in A$. Then

$$\chi(a) U_a V_\chi = V_\chi U_a \quad \forall \quad a \in A, \chi \in \hat{A}.$$

These are the Weyl commutation relations between the unitary operators representing A by translations and $\hat{A}$ by multiplications. The family of operators $\{U_a V_\chi \mid a \in A \chi \in \hat{A}\}$ is irreducible.

If $\mathbf{a} \in A^n$ then any element $\boldsymbol{\chi} \in \hat{A}^n$ can be identified with an element of $\hat{A}^n$ so that

$$\boldsymbol{\chi}(\mathbf{a}) = \prod_{i=1}^{n} \chi_i(a_i) \qquad \chi_i \in \hat{A}, a_i \in A$$

where $\boldsymbol{\chi} = (\chi_1, \ldots, \chi_n)$ and $\mathbf{a} = (a_1, \ldots, a_n)$. Put $U_{\mathbf{a}} = U_{a_1} \otimes \ldots \otimes U_{a_n}$ and $V_{\boldsymbol{\chi}} = V_{\chi_1} \otimes \ldots \otimes V_{\chi_n}$. Then $\{U_{\mathbf{a}} V_{\boldsymbol{\chi}} \mid \mathbf{a} \in A^n, \boldsymbol{\chi} \in \hat{A}^n\}$ is again an irreducible family of unitary operators satisfying the Weyl commutation relations

$$\boldsymbol{\chi}(\mathbf{a}) U_{\mathbf{a}} V_{\boldsymbol{\chi}} = V_{\boldsymbol{\chi}} U_{\mathbf{a}} \ \ \forall \ \ \mathbf{a} \in A^n, \boldsymbol{\chi} \in \hat{A}^n.$$

In the Hilbert space of all linear operators on $\mathcal{H}^{\otimes^n}$ equipped with the scalar product $\langle X \mid Y \rangle = TrX^{\dagger}Y$ the set $\{N^{-n/2} U_{\mathbf{a}} V_{\boldsymbol{\chi}} \mid \mathbf{a} \in A^n, \boldsymbol{\chi} \in \hat{A}^n\}$ is an orthonormal basis. The weight $wt(\mathbf{a}, \boldsymbol{\chi})$ of a pair $(\mathbf{a}, \boldsymbol{\chi}) \in A^n \times \hat{A}^n$ is defined to be $\#\{i \mid 1 \leq i \leq n, (a_i, \chi_i) \neq (0, 1)\}$, where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\boldsymbol{\chi} = (\chi_1, \ldots, \chi_n)$. The irreducibility of $\{U_{\mathbf{a}} V_{\boldsymbol{\chi}} \mid \mathbf{a} \in A^n, \boldsymbol{\chi} \in \hat{A}^n\}$ implies that $\{U_{\mathbf{a}} V_{\boldsymbol{\chi}} \mid \mathbf{a} \in A^n, \boldsymbol{\chi} \in \hat{A}^n, wt(\mathbf{a}, \boldsymbol{\chi}) \leq t\}$ spans $\mathcal{A}_t$. The Knill-Laflamme theorem for $\mathcal{A}_t$-correcting quantum codes assumes the following form which can be readily derived from Theorem 1.1.

Theorem 2.1 *$\mathcal{C}_n \subset L^2(A)^{\otimes^n}$ is a t-error correcting quantum code if and only if $\mathcal{C}_n$ has an orthonormal basis $\psi_1, \psi_2, \ldots, \psi_d$ satisfying the following conditions:*
For every $(\mathbf{a}, \boldsymbol{\chi}) \in A^n \times \hat{A}^n$ such that $wt(\mathbf{a}, \boldsymbol{\chi}) \leq 2t$

(i) $\langle \psi_i | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi_j \rangle = 0$ if $i \neq j$, and

(ii) $\langle \psi_i | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi_i \rangle$ is a scalar independent of ψ_i for $i = 1, 2, \ldots, d$.

Let l be the least positive integer such that $la = 0$ for all $a \in A$ and let $\omega = e^{\frac{2\pi i}{l}}$. We define the *error group* as the following finite group of unitary operators in $L^2(A)^{\otimes^n}$.

$$\mathcal{E} = \{\omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}} \mid 0 \leq i \leq l-1, \mathbf{a} \in A^n, \boldsymbol{\chi} \in \hat{A}^n\}.$$

The group $\mathcal{E}$ has a natural action on the Hilbert space $L^2(A)^{\otimes^n}$ defined by:

$$U_{\mathbf{a}} |\mathbf{x}\rangle = |\mathbf{x} + \mathbf{a}\rangle, \qquad\qquad V_{\boldsymbol{\chi}} |\mathbf{x}\rangle = \chi(\mathbf{x}) |\mathbf{x}\rangle.$$

Subspaces of $L^2(A)^{\otimes^n}$ that are point-wise fixed by some subgroup of the error group $\mathcal{E}$ are called *stabilizer codes*.

Let $\mathcal{S}$ be a subgroup of $\mathcal{E}$. Denote by $\mathcal{C}(\mathcal{S})$ the subspace of $L^2(A)^{\otimes^n}$ that is point-wise stabilized by $\mathcal{S}$. More precisely,

$$\mathcal{C}(\mathcal{S}) = \{\psi \in L^2(A)^{\otimes^n} \mid U\psi = \psi \ \ \forall \ \ U \in \mathcal{S}\}.$$

Lemma 2.2 *$\mathcal{C}(\mathcal{S}) \neq 0$ if and only if $\mathcal{S}$ is an abelian subgroup of $\mathcal{E}$ such that $\omega^i I \notin \mathcal{S}$ for $i \neq 0$. Furthermore, when $\mathcal{C}(\mathcal{S}) \neq 0$ the dimension of $\mathcal{C}(\mathcal{S})$ is $\#A^n / \#\mathcal{S}$.*

Proof. Suppose $\omega^i I \in \mathcal{S}$ for some $i \neq 0$. For any $\psi \in \mathcal{C}(\mathcal{S})$ we have $\omega^i I \psi = \psi$, which implies $\psi = 0$. Hence $\mathcal{C}(\mathcal{S}) = 0$.

It follows from the Weyl commutation relations that two elements $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\alpha}}$ and $\omega^j U_{\mathbf{b}} V_{\boldsymbol{\beta}}$ in $\mathcal{S}$ commute if and only if $\boldsymbol{\alpha}(\mathbf{b}) = \boldsymbol{\beta}(\mathbf{a})$. Now, let $\psi \in \mathcal{C}(\mathcal{S})$. We have

$$\psi = \omega^i U_{\mathbf{a}} V_{\boldsymbol{\alpha}} \omega^j U_{\mathbf{b}} V_{\boldsymbol{\beta}} \psi = \omega^j U_{\mathbf{b}} V_{\boldsymbol{\beta}} \omega^i U_{\mathbf{a}} V_{\boldsymbol{\alpha}} \psi.$$

Applying the commutation relations we can see that the above equation holds for a $\psi \neq 0$ if and only if $\boldsymbol{\alpha}(\mathbf{b}) = \boldsymbol{\beta}(\mathbf{a})$. Thus, $\mathcal{C}(\mathcal{S}) \neq 0$ if and only if $\mathcal{S}$ is abelian and $\omega^i I \notin \mathcal{S}$ for $i \neq 0$.

Now, let $\mathcal{S}$ be an abelian subgroup of $\mathcal{E}$ such that $\omega^i I \notin \mathcal{S}$ for $i \neq 0$. Define the projection operator

$$P = \frac{1}{\#\mathcal{S}} \sum_{U \in \mathcal{S}} U.$$

Since $\mathit{Tr} U_{\mathbf{a}} V_{\boldsymbol{\beta}} = 0$ unless $(\mathbf{a}, \boldsymbol{\beta}) = (0, 1)$ it follows that $\mathit{Tr}(P) = \#A^n/\#\mathcal{S}$. It is easy to see that P is the projection onto $\mathcal{C}(\mathcal{S})$. Thus, the dimension of $\mathcal{C}(\mathcal{S})$ is $\mathit{Tr}(P) = \#A^n/\#\mathcal{S}$. This completes the proof. ∎

Next, we state Theorem 2.1 in a form that will give the criteria for constructing t-error correcting quantum stabilizer codes. Let $Z(\mathcal{S})$ denote the centralizer of $\mathcal{S}$ in $\mathcal{E}$, i.e.,

$$Z(\mathcal{S}) = \{U \in \mathcal{E} \mid UU' = U'U \quad \forall \quad U' \in \mathcal{S}\}.$$

Theorem 2.3 *Let $\mathcal{S}$ be an abelian subgroup of the error group $\mathcal{E}$ such that $\omega^i I$ is not in $\mathcal{S}$ for $i \neq 0$. Then $\mathcal{C}(\mathcal{S})$ is a t-error correcting quantum code if $wt(\mathbf{a}, \boldsymbol{\alpha}) > 2t$ for each $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\alpha}} \in Z(\mathcal{S}) \setminus \mathcal{S}$.*

Proof. Suppose $wt(\mathbf{a}, \boldsymbol{\alpha}) > 2t$ for each $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\alpha}} \in Z(\mathcal{S}) \setminus \mathcal{S}$. Now, by the previous lemma $\mathcal{C}(\mathcal{S})$ is a subspace of $L^2(A)^{\otimes^n}$ of dimension $\#A^n/\#\mathcal{S} = d$. Let $\psi_1, \ldots, \psi_d$ be an orthonormal basis of $\mathcal{C}(\mathcal{S})$. Consider a $(\mathbf{a}, \boldsymbol{\chi}) \in A^n \times \hat{A}^n$ with the property that $wt(\mathbf{a}, \boldsymbol{\chi}) \leq 2t$. We check the Knill-Laflamme conditions (Theorem 2.1). There are two cases:

(a) If $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}} \in \mathcal{S}$ for some $i \geq 0$ then

$$\langle \psi_j | \omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi_k \rangle = \langle \psi_j \mid \psi_k \rangle = \delta_{jk}, \quad 1 \leq j, k \leq d.$$

Thus, $\langle \psi_j | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi_k \rangle = \omega^{-i} \delta_{jk} 1 \leq j, k \leq d$, where δ_{jk} is the Kronecker delta function.

(b) If $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}} \notin \mathcal{S}$ for each $i \geq 0$, then since $wt(\mathbf{a}, \boldsymbol{\chi}) \leq 2t$, $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}} \notin Z(\mathcal{S})$ for each $i \geq 0$ by the assumption. Let $\psi \in \mathcal{C}(\mathcal{S})$ and $\omega^r U_{\mathbf{b}} V_{\boldsymbol{\beta}}$ be some element of $\mathcal{S}$. Then we can write $\langle \psi | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi \rangle$ as $\langle \omega^r U_{\mathbf{b}} V_{\boldsymbol{\beta}} \psi | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \omega^r U_{\mathbf{b}} V_{\boldsymbol{\beta}} \psi \rangle$, which can be simplified to get the following

$$\langle \psi | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi \rangle = \overline{\boldsymbol{\beta}(\mathbf{a})} \boldsymbol{\chi}(\mathbf{b}) \langle \psi | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi \rangle. \tag{2}$$

Since $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}} \notin Z(\mathcal{S})$ for each $i \geq 0$, for some $\omega^r U_{\mathbf{b}} V_{\boldsymbol{\beta}} \in \mathcal{S}$ we must have $\boldsymbol{\beta}(\mathbf{a}) \neq \boldsymbol{\chi}(\mathbf{b})$. This choice of $\omega^r U_{\mathbf{b}} V_{\boldsymbol{\beta}} \in \mathcal{S}$ yields $\langle \psi | U_{\mathbf{a}} V_{\boldsymbol{\chi}} | \psi \rangle = 0$.

∎

At this point it is useful to introduce a standard notation using which it is convenient to describe quantum stabilizer codes. Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{E}$ with centralizer $Z(\mathcal{S})$. The *minimum distance* $d(\mathcal{S})$ is defined to be the minimum of

$$\{wt(\mathbf{a}, \boldsymbol{\alpha}) \mid \omega^i U_{\mathbf{a}} V_{\boldsymbol{\alpha}} \in Z(\mathcal{S}) \setminus \mathcal{S}\}.$$

When A is the additive abelian group of the finite field $\mathbb{F}_q$ we define an $[[n,k,d]]_q$ quantum stabilizer code to be a q^k-dimensional subspace $\mathcal{C}(\mathcal{S})$ of $L^2(\mathbb{F}_q)^{\otimes^n}$, where $\mathcal{S}$ is an abelian subgroup of $\mathcal{E}$ with $d(\mathcal{S}) \geq d$ and cardinality q^{n-k}.

By Theorem 2.3 it follows that an $[[n,k,d]]_q$ quantum stabilizer code is a $\lfloor (d-1)/2 \rfloor$-error correcting quantum code.

Remark 2.4 *Let $\mathcal{S}$ be an abelian subgroup of $\mathcal{E}$ such that $\omega^i I \notin \mathcal{S}$ for every $i \neq 0$. This is equivalent to demanding that $\mathcal{S}$ is an abelian subgroup of $\mathcal{E}$ such that for any $\mathbf{a} \in A^n$ and $\boldsymbol{\chi} \in \hat{A}^n$ the operator $\omega^i U_{\mathbf{a}} V_{\boldsymbol{\chi}}$ can be in $\mathcal{S}$ for at most one $i : 0 \leq i \leq l-1$, Thus $\mathcal{S}$ has the form*

$$\mathcal{S} = \{p(\mathbf{a}, \boldsymbol{\chi}) U_{\mathbf{a}} V_{\boldsymbol{\chi}} \mid (\mathbf{a}, \boldsymbol{\chi}) \in S\}$$

where $S \subset A^n \times \hat{A}^n$ is a subgroup satisfying $\boldsymbol{\chi}(\mathbf{a}') = \boldsymbol{\chi}'(\mathbf{a})$ for any $(\mathbf{a}, \boldsymbol{\chi}), (\mathbf{a}'\boldsymbol{\chi}') \in \mathcal{S}$ and p is a function on S with values in $\{\omega^i \mid 0 \leq i \leq l-1\}$.

3 Quantum stabilizer codes in the finite field setting

In order to construct stabilizer quantum codes, we need to study abelian subgroups $\mathcal{S}$ of $\mathcal{E}$ such that elements in $Z(\mathcal{S}) \setminus \mathcal{S}$ have large weight. We choose A to be a finite field $\mathbb{F}_q$, $q = p^r$ for some prime p. In particular, the Hilbert space in which we seek stabilizer codes is $L^2(\mathbb{F}_q)^{\otimes^n}$. Since $\mathbb{F}_q$ is an abelian group under its addition operation with each nonzero element of order p, it follows that every nontrivial character of $\mathbb{F}_q$ is of order p. Choose a nontrivial character $\tilde{\omega} \in \hat{F}_q$. Then every other character $\omega' \in \hat{\mathbb{F}}_q$ is of the form ω_a where $\omega_a(x) = \tilde{\omega}(ax)$ for all $x \in \mathbb{F}_q$. Likewise, every character in $\hat{\mathbb{F}}_q^{\,n}$ is of the form $\omega_{\mathbf{a}}$ where $\omega_{\mathbf{a}}(\mathbf{x}) = \tilde{\omega}(\mathbf{a} \cdot \mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_q^n$, where $\mathbf{a} \cdot \mathbf{x}$ is the inner product $\sum_i a_i x_i$, for $\mathbf{a} = (a_1, \ldots, a_n)^T$ and $\mathbf{x} = (x_1, \ldots, x_n)^T$.

If we identify $\hat{\mathbb{F}}_q^{\,n}$ with $\mathbb{F}_q^n$, we can index the elements of the error group $\mathcal{E}$ as $\omega^i U_{\mathbf{a}} V_{\mathbf{b}}$, $0 \leq i \leq p-1$, and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, where $V_{\mathbf{b}}$ now stands for the operator $V_{\boldsymbol{\chi}}$ with $\boldsymbol{\chi} = \omega_{\mathbf{b}}$. Thus, $\mathcal{E}$ is rewritten as

$$\mathcal{E} = \{\omega^i U_{\mathbf{a}} V_{\mathbf{b}} \mid 0 \leq i \leq p-1, \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}.$$

Notice that $\mathcal{E}$ is a finite group of cardinality pq^{2n}. The Weyl commutation relations take the following form

$$\tilde{\omega}(\mathbf{b} \cdot \mathbf{a}) U_{\mathbf{a}} V_{\mathbf{b}} = V_{\mathbf{b}} U_{\mathbf{a}} \ \ \forall \ \ \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n.$$

If $\mathcal{S}$ is a subgroup of $\mathcal{E}$ it is readily seen that $\mathcal{S}$ is abelian if and only if for any two elements $\omega^i U_{\mathbf{a}} V_{\mathbf{b}}$ and $\omega^j U_{\mathbf{c}} V_{\mathbf{d}}$ in $\mathcal{S}$ we have $\mathbf{a} \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{c}$. For $(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$, define $wt(\mathbf{a}, \mathbf{b}) = \#\{i \mid (a_i, b_i) \neq (0,0)\}$, where $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$. Let $S \subset \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a subgroup for which $\mathbf{a} \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{c}$ for all $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in S$. Define

$$S^{\perp_s} = \{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \mid \mathbf{a} \cdot \mathbf{d} - \mathbf{b} \cdot \mathbf{c} = 0 \text{ for all } (\mathbf{c}, \mathbf{d}) \in \mathcal{S}\}.$$

Lemma 2.2 and the Knill-Laflamme conditions can be restated as follows.

Lemma 3.1 *Let $S \subset \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a subgroup for which $\mathbf{a} \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{c}$ for all $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in S$. Suppose $\tilde{p} : S \to \{\omega^i \mid 0 \leq i \leq p-1\}$ is a function such that $\mathcal{S} = \{\tilde{p}(\mathbf{a}, \mathbf{b}) U_{\mathbf{a}} V_{\mathbf{b}} \mid (\mathbf{a}, \mathbf{b}) \in S\}$*

is an abelian subgroup of $\mathcal{E}$. Then $\mathcal{C}(\mathcal{S}) \subset L^2(\mathbb{F}_q)^{\otimes n}$ is a quantum stabilizer code of dimension $q^n/\#S$. Furthermore, if $wt(\mathbf{a}, \mathbf{b}) > 2t$ for all nonzero elements $(\mathbf{a}, \mathbf{b}) \in S^{\perp_s} \setminus S$ then $\mathcal{C}(\mathcal{S})$ is a t-error correcting quantum stabilizer code.

Thus the problem is to find subgroups S of $\mathbb{F}_q^n \times \mathbb{F}_q^n$ such that $\mathbf{a} \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{c}$ for all $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in S$ and $wt(\mathbf{a}, \mathbf{b})$ is large for nonzero elements $(\mathbf{a}, \mathbf{b}) \in S^{\perp_s} \setminus S$. The other problem is to ensure that we can build an abelian subgroup $\mathcal{S}$ of $\mathcal{E}$ by picking a suitable $\tilde{p} : S \to \{\omega^i \mid 0 \le i \le p-1\}$ such that $\mathcal{S} = \{\tilde{p}(\mathbf{a}, \mathbf{b}) U_{\mathbf{a}} V_{\mathbf{b}} \mid (\mathbf{a}, \mathbf{b}) \in S\}$. To this end, we formulate an approach.

Let $\mathcal{V}$ be an m-dimensional vector space over $\mathbb{F}_q$ for a positive integer m. Let $L : \mathcal{V} \to \mathbb{F}_q^n$ and $M : \mathcal{V} \to \mathbb{F}_q^n$ be two linear transformations. Thus, L and M can be written as $n \times m$ matrices over $\mathbb{F}_q$. We restrict attention to abelian subgroups of $\mathcal{E}$ that are of the form

$$\{\tilde{p}(\mathbf{v}) U_{L\mathbf{v}} V_{M\mathbf{v}} \mid \mathbf{v} \in \mathcal{V}\}.$$

Two elements $\tilde{p}(\mathbf{v}_1) U_{L\mathbf{v}_1} V_{M\mathbf{v}_1}$, $\tilde{p}(\mathbf{v}_2) U_{L\mathbf{v}_2} V_{M\mathbf{v}_2}$ commute precisely when

$$\mathbf{v}_2^T L^T M \mathbf{v}_1 = \mathbf{v}_1^T L^T M \mathbf{v}_2 \quad \forall \quad \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V} \tag{3}$$

and

$$\frac{\tilde{p}(\mathbf{v}_1 + \mathbf{v}_2)}{\tilde{p}(\mathbf{v}_1)\tilde{p}(\mathbf{v}_2)} = \tilde{\omega}(\mathbf{v}_2^T L^T M \mathbf{v}_1) = \tilde{\omega}(\mathbf{v}_1^T L^T M \mathbf{v}_2) \quad \forall \quad \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}. \tag{4}$$

Equation (3) will hold if we choose L and M such that $M^T L = L^T M$ (i.e. L and M are such that $M^T L$ is symmetric).

Writing $\tilde{p}(\mathbf{v}) = \tilde{\omega}(\tilde{q}(\mathbf{v}))$, for some function $\tilde{q} : \mathcal{V} \to \mathbb{F}_q$, Equation (4) assumes the form

$$\tilde{q}(\mathbf{v}_1 + \mathbf{v}_2) - \tilde{q}(\mathbf{v}_1) - \tilde{q}(\mathbf{v}_2) = \mathbf{v}_2^T L^T M \mathbf{v}_1 = \mathbf{v}_1^T L^T M \mathbf{v}_2 \quad \forall \quad \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}.$$

For $p \neq 2$ we can choose $\tilde{q}$ to be the quadratic form $\frac{1}{2}\mathbf{v}^T M^T L \mathbf{v}$. For $p = 2$ the problem of recovering a suitable quadratic form as a solution to the above equation is more difficult.

For the purpose of this article, we look for special solutions: we demand that $L^T M$ be expressible as $D + D^T$ for some matrix D over $\mathbb{F}_q$, which implies that $L^T M$ is a symmetric matrix with diagonal entries as scalar multiples of 2. For example, we can choose D to be an upper diagonal matrix. Then $q(\mathbf{v}) = \mathbf{v}^T D \mathbf{v}$ is a solution to Equation (4). We summarize this below.

Lemma 3.2 *Let $\mathcal{V}$ be a finite dimensional vector space, and $L : \mathcal{V} \to \mathbb{F}_q^n$ and $M : \mathcal{V} \to \mathbb{F}_q^n$ be two linear transformations such that $M^T L$ is symmetric and of the form $D + D^T$ for a linear map $D : \mathcal{V} \to \mathbb{F}_q^n$. Then*

$$\mathcal{S} = \{\tilde{\omega}(\mathbf{v}^T D \mathbf{v}) U_{L\mathbf{v}} V_{M\mathbf{v}} \mid \mathbf{v} \in \mathcal{V}\}$$

is an abelian subgroup of the error group $\mathcal{E}$ on $L^2(\mathbb{F}_q)^{\otimes n}$.

An element $\omega^i U_{\mathbf{x}} V_{\mathbf{y}}$ of $\mathcal{E}$ is in $Z(\mathcal{S})$ if and only if $\mathbf{v}^T M^T \mathbf{x} = \mathbf{v}^T L^T \mathbf{y}$ for all $\mathbf{v} \in \mathcal{V}$. Equivalently, $\omega^i U_{\mathbf{x}} V_{\mathbf{y}} \in Z(\mathcal{S})$ if and only if $M^T \mathbf{x} = L^T \mathbf{y}$.

From the Knill-Laflamme conditions as stated in Theorem 2.3, $\mathcal{C}(\mathcal{S})$ is a t-error correcting quantum code with $\mathcal{S}$ defined as above if for any $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$, the condition $M^T \mathbf{x} = L^T \mathbf{y}$ implies that either $\mathbf{x} = L\mathbf{v}$ and $\mathbf{y} = M\mathbf{v}$ for some $\mathbf{v} \in \mathcal{V}$ or $wt(\mathbf{x}, \mathbf{y}) > 2t$.

If $\mathbb{F}_q$ has characteristic different from 2 there is a partial converse to Lemma 3.2: Suppose $\mathcal{C}(\mathcal{S})$ is some stabilizer code in $L^2(\mathbb{F}_q)^{\otimes^n}$ where $\mathcal{S} = \{\tilde{p}(\mathbf{a}, \mathbf{b}) U_{\mathbf{a}} V_{\mathbf{b}} \mid (\mathbf{a}, \mathbf{b}) \in \mathcal{S}\}$ for some additive subgroup S such that $\mathbf{a} \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{c}$ for all $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in S$. Let $\#S = q^r$ and $(\mathbf{a}_1 \mathbf{b}_1), (\mathbf{a}_2, \mathbf{b}_2) \ldots, (\mathbf{a}_r \mathbf{b}_r)$ be an independent generating set for S. Then $S_1 = \{\mathbf{a} \in \mathbb{F}_q^n \mid \exists \mathbf{b} \in \mathbb{F}_q^n \ : \ (\mathbf{a}, \mathbf{b}) \in S\}$ and $S_2 = \{\mathbf{b} \in \mathbb{F}_q^n \mid \exists \mathbf{a} \in \mathbb{F}_q^n \ : \ (\mathbf{a}, \mathbf{b}) \in S\}$ are linear subspaces of $\mathbb{F}_q^n$. Let $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r$ be the standard basis for $\mathbb{F}_q^r$. Define $L : \mathbb{F}_q^r \to \mathbb{F}_q^n$ and $M : \mathbb{F}_q^r \to \mathbb{F}_q^n$ by letting $L\mathbf{e}_i = \mathbf{a}_i$ and $M\mathbf{e}_i = \mathbf{b}_i$ for $i = 1, 2, \ldots, r$. Since , $\mathbf{a} \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{c}$ for all $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{d}) \in S$, it follows that $L^T M$ is symmetric. Suppose $\mathbb{F}_q$ is of characteristic $p \neq 2$. For $(\mathbf{a}, \mathbf{b}) \in S$, let $\mathbf{v} \in \mathbb{F}_q^r$ be such that $L\mathbf{v} = \mathbf{a}$ and $M\mathbf{v} = \mathbf{b}$ and define $p'(\mathbf{v}) = \frac{1}{2}\mathbf{v}^T L^T M \mathbf{v}$. It is easy to check that $p(\mathbf{a}, \mathbf{b}) = p'(\mathbf{v}) + \mathbf{c} \cdot \mathbf{v}$, for some $\mathbf{c} \in \mathbb{F}_q^r$. More precisely, we have the following proposition.

Proposition 3.3 *Suppose $\mathbb{F}_q$ has characteristic different from 2 and $\mathcal{C}(\mathcal{S})$ is some stabilizer code in $L^2(\mathbb{F}_q)^{\otimes^n}$ of dimension q^{n-r}. Then there are linear transformations $L : \mathbb{F}_q^r \to \mathbb{F}_q^n$ and $M : \mathbb{F}_q^r \to \mathbb{F}_q^n$ such that $L^T M$ is symmetric and there is a $\mathbf{c} \in \mathbb{F}_q^n$ such that $\mathcal{S} = \{\tilde{\omega}(\frac{1}{2}\mathbf{v}^T L^T M \mathbf{v} + \mathbf{c} \cdot \mathbf{v}) U_{L\mathbf{v}} V_{M\mathbf{v}} \mid \mathbf{v} \in \mathbb{F}_q^r\}$.*

We can derive the following proposition from Lemma 3.2.

Proposition 3.4 *Let $L : \mathbb{F}_q^{n-1} \to \mathbb{F}_q^n$ be an injective linear map with range $C = \{\mathbf{a} \in \mathbb{F}_q^n \mid \sum_{i=1}^n a_i = 0\}$ and $M = M'L$ for some symmetric linear map $M' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ of the form $M' = D + D^T$. Then*

(i) $\mathcal{S} = \{\tilde{\omega}(\mathbf{a}^T D \mathbf{a}) U_{\mathbf{a}} V_{M'\mathbf{a}} \mid \mathbf{a} \in C\}$ is an abelian subgroup of $\mathcal{E}$.

(ii) $\mathcal{C}(\mathcal{S})$ is t-error correcting if for any $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$, the condition $\mathbf{y} - M'\mathbf{x} \in C^\perp$ implies that either $\mathbf{x} \in C$ and $\mathbf{y} = M'\mathbf{x}$ or $wt(\mathbf{x}, \mathbf{y}) > 2t$.

Let $\mathcal{S} = \{\tilde{\omega}(\mathbf{a}^T D \mathbf{a}) U_{\mathbf{a}} V_{L\mathbf{a}} \mid \mathbf{a} \in C\}$, where $L = D + D^T$, L and D are $n \times n$ matrices over $\mathbb{F}_q$, and C is a subspace of $\mathbb{F}_q^n$. As already observed $\mathcal{S}$ is an abelian subgroup of $\mathcal{E}$. Our next goal is to give an orthonormal basis for $\mathcal{C}(\mathcal{S})$. Notice that $\mathcal{C}(\mathcal{S})$ is a $q^n/\#C$-dimensional subspace of $L^2(\mathbb{F}_q)^{\otimes^n}$. Since C is an additive subgroup of $\mathbb{F}_q^n$, it suggests that an orthonormal basis for $\mathcal{C}(\mathcal{S})$ can be indexed by the cosets of C in $\mathbb{F}_q^n$. It suffices to describe unit vectors $|\psi_{C+\mathbf{x}}\rangle \in L^2(\mathbb{F}_q)^{\otimes^n}$ that have disjoint support in $\mathbb{F}_q^n$, and show that each $|\psi_{C+\mathbf{x}}\rangle$ is fixed by $\mathcal{S}$, where $\mathbf{x}$ runs over a set of distinct coset representatives of C in $\mathbb{F}_q^n$. Define

$$|\psi_{C+\mathbf{x}}\rangle = \frac{1}{\sqrt{\#C}} \sum_{\mathbf{a} \in C} \tilde{\omega}(\mathbf{a}^T D \mathbf{a}) \tilde{\omega}(\mathbf{a}^T L \mathbf{x}) |\mathbf{a} + \mathbf{x}\rangle \tag{5}$$

for each coset $C + \mathbf{x}$ as $\mathbf{x}$ runs over a set of distinct coset representatives of C in $\mathbb{F}_q^n$. The vectors $|\psi_{C+\mathbf{x}}\rangle$ have unit norm, and as they have mutually disjoint supports, they form an orthonormal set of $q^n/\#C$ vectors in $L^2(\mathbb{F}_q)^{\otimes^n}$. It can be easily verified that $\mathcal{S}$ fixes each $|\psi_{C+\mathbf{x}}\rangle$. We summarize or observations below.

Proposition 3.5 *Let* $\mathcal{S} = \{\tilde{\omega}(\mathbf{a}^T D\mathbf{a})U_{\mathbf{a}}V_{L\mathbf{a}} \mid \mathbf{a} \in C\}$*, where* $L = D + D^T$*,* L *and* D *are* $n \times n$ *matrices over* $\mathbb{F}_q$*, and* C *is a subspace of* $\mathbb{F}_q^n$*. Then the collection of vectors* $\{|\psi_{C+\mathbf{x}}\rangle\}$ *defined as*

$$|\psi_{C+\mathbf{x}}\rangle = \frac{1}{\sqrt{\#C}} \sum_{\mathbf{a}\in C} \tilde{\omega}(\mathbf{a}^T D\mathbf{a})\tilde{\omega}(\mathbf{a}^T L\mathbf{x})|\mathbf{a}+\mathbf{x}\rangle$$

for each coset $C + \mathbf{x}$ *as* $\mathbf{x}$ *runs over a set of distinct coset representatives of* C *in* $\mathbb{F}_q^n$*, is an orthonormal basis for* $\mathcal{C}(\mathcal{S})$*. In particular,* $\dim \mathcal{C}(\mathcal{S}) = q^{n-\dim C}$.

Remark 3.6 $\mathcal{C}(\mathcal{S})$ *is an* $[[n, k, d]]_q$ *quantum code if it has dimension* q^k *and* $d(\mathcal{S}) \geq d$*. In line with classical coding theory we can define the* rate *of an* $[[n, k, d]]_q$ *quantum code as* k/n *and* relative distance *as* d/n*. It is clearly desirable to design quantum codes with large rates and relative distance. An* $[[n, k, d]]_q$ *quantum code* $\mathcal{C}(\mathcal{S})$ *is a* pure *code if the corresponding centralizer subgroup* $Z(\mathcal{S})$ *has the property that* $wt(\mathbf{a}, \mathbf{b}) \geq d$ *for each* $\omega^i U_{\mathbf{a}} V_{\mathbf{b}} \in Z(\mathcal{S})$*,* $(\mathbf{a}, \mathbf{b}) \neq (0, 0)$*. (Notice that this is a stronger property than guaranteed by Theorem 2.3). Given a pure quantum stabilizer code, the following simple method can be used for deriving new quantum codes.*

Suppose we have an $[[n, k, d]]_q$ *pure quantum code, with a small* k *and large* d*. From such a code we can construct an* $[[n-1, k+1, d-1]]_q$ *quantum code that is again pure, by the technique of puncturing* S *to yield an additive subgroup* S' *of* $\mathbb{F}_q^{n-1} \times \mathbb{F}_q^{n-1}$*, of size still* q^{n-k} *and distance at least* $d(\mathcal{S}) - 1$*. The idea of punctured classical codes (see McWilliams and Sloane [8]) can be adapted to punctured pure quantum stabilizer codes following [2] where it is shown for* $q = 2$*. A repeated application of puncturing will give* $[[n-k', k+k', d-k']]_q$ *codes for different choices of* k'*.*

4 A class of stabilizer codes

First choose and fix the following subspace C of $\mathbb{F}_q^n$:

$$C = \{(a_1, \ldots, a_n)^T \in \mathbb{F}_q^n \mid \sum_i a_i = 0\}.$$

The subspace C is invariant under the cyclic shift permutation $\sigma : i \mapsto (i+1) mod\ n$. Thus, $C^\perp = \{(a, \ldots, a) \in \mathbb{F}_q^n \mid a \in \mathbb{F}_q\}$ is also invariant under σ. An $n \times n$ matrix L over $\mathbb{F}_q$ is said to be *circulant* if for $i = 2, \ldots, n$, the i^{th} row of L is obtained by applying σ^{i-1} to the first row.

Let $\mathcal{S} = \{\tilde{\omega}(\mathbf{a}^T D\mathbf{a})U_{\mathbf{a}}V_{L\mathbf{a}} \mid \mathbf{a} \in C\}$, where $L = D + D^T$ is an $n \times n$ matrix over $\mathbb{F}_q$ and C is as chosen above. We further specialize our construction by choosing L to be an $n \times n$ symmetric circulant matrix with entries from $\{0, 1\}$ and with all diagonal entries 0. Let $\mathbf{e}_1 = (1, 0, \ldots, 0) \in \mathbb{F}_q^n$. For such an L observe that $\mathbf{a}^T L\mathbf{e}_1 = \mathbf{a}^T D^T \mathbf{e}_1$ for $\mathbf{a} \in C$. Then the orthonormal basis $\{|\psi_{C+\mathbf{x}}\rangle\}$ for $\mathcal{C}(\mathcal{S})$ (as described in Equation (5)) can be written in the following form:

$$|\psi_{C+c\mathbf{e}_1}\rangle = \frac{1}{\sqrt{\#C}} \sum_{\mathbf{a}\in C} \tilde{\omega}((\mathbf{a}^T + c\mathbf{e}_1^T)D(\mathbf{a} + c\mathbf{e}_1))|\mathbf{a} + c\mathbf{e}_1\rangle, \quad \mathbf{c} \in \mathbb{F}_q. \tag{6}$$

In particular, for $q = 2$ the above stabilizer code has a neat encoding circuit that we describe in Figure **??** in the appendix.

As an example of stabilizer codes given by Equation (6), we now describe a $[[5, 1, 3]]_q$ quantum code for every finite field $\mathbb{F}_q$. In particular, for $q = 2$, the $[[5, 1, 3]]_2$ code is the Laflamme code which was originally obtained by a computer search [6]. Let L_5 be the following symmetric circulant matrix in $\mathbb{F}_q^{5\times 5}$.

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

and $C = \{(a_1, \ldots, a_5)^T \in \mathbb{F}_q^5 \mid \sum_i a_i = 0\}$. It can be checked that $S = \{(\mathbf{a}, L_5\mathbf{a}) \mid \mathbf{a} \in C\}$ is an additive subgroup of $\mathbb{F}_q^5 \times \mathbb{F}_q^5$ such that $d(\mathcal{S}) \geq 3$. Thus, by Theorem 2.3, $\mathcal{C}(\mathcal{S})$ is a $[[5, 1, 3]]_q$ quantum code for every finite field $\mathbb{F}_q$. The encoding circuit for the $[[5, 1, 3]]_2$ can be obtained easily from the general encoding circuit already described for codes given by Equation (6).

For a vector $\mathbf{c} \in \mathbb{F}_2^n$, let $\sigma\mathbf{c} \in \mathbb{F}_2^n$ denote the vector obtained by a cyclic shift of $\mathbf{c}$. An $n \times n$ circulant matrix with first column $\mathbf{c} \in \mathbb{F}_2^n$ can be conveiently written as

$$\begin{pmatrix} \mathbf{c} & \sigma\mathbf{c} & \ldots & \sigma^{n-1}\mathbf{c} \end{pmatrix}$$

We give two more examples of quantum codes defined using circulant matrices.

First, there is a $[[13, 1, 5]]_2$ quantum code defined by a 13×13 circulant matrix L_{13} over $\mathbb{F}_2$, whose first column is

$$\mathbf{c} = (0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0)^T.$$

As defined, $C = \{(a_1, \ldots, a_{13})^T \in \mathbb{F}_2^{13} \mid \sum_i a_i = 0\}$. It can be checked (with the help of a computer program) that $S = \{(\mathbf{a}, L_{13}\mathbf{a}) \mid \mathbf{a} \in C\}$ is an additive subgroup of $\mathbb{F}_2^{13} \times \mathbb{F}_q^{13}$ such that $d(\mathcal{S}) \geq 5$. Thus, by Theorem 2.3, $\mathcal{C}(\mathcal{S})$ is a pure $[[13, 1, 5]]_2$ quantum code.

Similarly, there is a $[[21, 1, 7]]_2$ quantum code defined by a 21×21 circulant matrix L_{21} over $\mathbb{F}_2$, whose first column is

$$\mathbf{c} = (0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1)^T$$

As before, $C = \{(a_1, \ldots, a_{21})^T \in \mathbb{F}_2^{21} \mid \sum_i a_i = 0\}$. It can be checked using a computer program that $S = \{(\mathbf{a}, L_{21}\mathbf{a}) \mid \mathbf{a} \in C\}$ is an additive subgroup of $\mathbb{F}_2^{21} \times \mathbb{F}_q^{21}$ such that $d(\mathcal{S}) \geq 7$. Thus, by Theorem 2.3, $\mathcal{C}(\mathcal{S})$ is a pure $[[21, 1, 7]]_2$ quantum code.

If $k = 1$, it is interesting to note that for $n = 5, 13$ and 21, the best achievable minimum distance [2] is $d = 3, 5,$ and 7 respectively.

5 Existence of good stabilizer codes

Using a probabilistic argument we show that there is a number $\alpha > 0$ and a natural number n_α such that for each $n > n_\alpha$ there exists a $[[n, 1, \lfloor \alpha n \rfloor]]_2$ pure quantum stabilizer code. Now, as observed in Remark 3.6, given β such that $0 < \beta < \alpha$, by the method of punctured codes we can obtain a family of $[[\lfloor(1-\beta)n\rfloor, \lfloor\beta n\rfloor, \lfloor(\alpha-\beta)n\rfloor]]_2$ quantum codes for all $n > n_\alpha$. These are good quantum codes with constant rate $\beta/(1-\beta)$ and constant relative distance $(\alpha-\beta)/(1-\beta)$.

We first recall a particular form of the Chernoff bounds for bounding the probability that a random variable deviates far from its expectation.

Theorem 5.1 [9, Theorem 4.2, page 70] *Let $X_1, X_2, \ldots, X_n$ be independent Bernoulli random variables such that for each i, $\Pr[X_i = 1] = p$ and $\Pr[X_i = 0] = 1 - p$, for $0 < p < 1$. Let $X = \sum_i X_i$ and let μ denote the expectation $\mathbf{E}[X]$. Then for $0 < \delta < 1$*

$$\Pr[X < (1-\delta)\mu] < e^{-\mu\delta^2/2}.$$

Our existence proof for stabilizer codes will be guided by Lemma 3.2.

As before, we first choose and fix the following subspace C of $\mathbb{F}_q^n$:

$$C = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid \sum_i a_i = 0\}.$$

Definition 5.2 *An $n \times n$ matrix R over $\mathbb{F}_2$ is said to be α-*good *if the following conditions are true.*

(i) The sum of every $\lfloor\alpha n\rfloor$ columns of R has weight at least αn.

(ii) The sum of every $\lfloor\alpha n\rfloor$ rows of R has weight at least αn.

(iii) The sum of every $\lfloor\alpha n\rfloor$ columns of R has weight at most $(1-\alpha)n$.

(iv) The sum of every $\lfloor\alpha n\rfloor$ rows of R has weight at most $(1-\alpha)n$.

As in classical coding theory [8], given a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)^T \in \mathbb{F}_q^n$ we denote $\#\{i \mid a_i \neq 0\}$ by $w(\mathbf{a})$. The next proposition describes a way of constructing stabilizer codes from good matrices.

Theorem 5.3 *For $0 < \alpha < 1$, suppose R is an $n \times n$ α-good matrix over $\mathbb{F}_2$. Let L be the following $2n \times 2n$ symmetric matrix over $\mathbb{F}_2$:*

$$\begin{pmatrix} 0 & R \\ R^T & 0 \end{pmatrix}$$

If we write $L = D + D^T$, where D is the upper triangular matrix with zeros on the principal diagonal, and define the abelian subgroup $\mathcal{S}$ of $\mathcal{E}$ as $\mathcal{S} = \{\tilde{\omega}(\mathbf{a}^T D\mathbf{a})U_{\mathbf{a}}V_{L\mathbf{a}} \mid \mathbf{a} \in C\}$, then $\mathcal{C}(\mathcal{S})$ is a $[[2n, 1, \lfloor\alpha n\rfloor]]_2$ pure stabilizer code.

Proof. From Lemma 3.2, we know that $\mathcal{C}(\mathcal{S})$ is a $[[2n, 1, \lfloor \alpha n \rfloor]]_2$ stabilizer code if for any $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$, the condition $\mathbf{y} - L\mathbf{x} \in C^{\perp}$ implies that either $\mathbf{x} \in C$ and $\mathbf{y} = L\mathbf{x}$ or $wt(\mathbf{x}, \mathbf{y}) > \alpha n$. It is easy to check that the assumptions about R in Definition 5.2, in fact, guarantees a stronger property: for any nonzero vector $\mathbf{x} \in \mathbb{F}_2^n$ such that $w(\mathbf{x}) \leq \alpha n$, the assumptions (i) and (iii) imply that $\alpha n \leq w(R\mathbf{x}) \leq (1 - \alpha)n$. Similarly, assumptions (ii) and (iv) imply that $\alpha n \leq w(R^T\mathbf{x}) \leq (1 - \alpha)n$. Putting these together, it follows that $\alpha n \leq w(L\mathbf{x}) \leq (1 - \alpha)n$ if $w(\mathbf{x}) \leq \alpha n$ for $\mathbf{x} \in \mathbb{F}_2^{2n}$.

Since $C^{\perp} = \{(1, 1, \ldots, 1)^T, (0, 0, \ldots, 0)^T\}$, we can see that the above observation implies that $wt(\mathbf{x}, \mathbf{y}) > \alpha n$ if $(0, 0) \neq (\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$, and $\mathbf{y} - L\mathbf{x} \in C^{\perp}$. It follows that $\mathcal{C}(\mathcal{S})$ is a $[[2n, 1, \lfloor \alpha n \rfloor]]_2$ pure stabilizer code. This completes the proof. ■

We now show the existence of $n \times n$ matrices over $\mathbb{F}_2$ that fulfill the conditions of Theorem 5.3.

Lemma 5.4 *Let R_{ij}, $1 \leq i, j \leq n$ be independent identically distributed random variables taking values in $\{0, 1\}$ such that $\Pr[R_{ij} = 1] = 1/2$, $1 \leq i, j \leq n$. Let R be the uniformly distributed $n \times n$ random matrix over $\mathbb{F}_2$ whose ij^{th} entry is the random variable R_{ij}. There exist constants $\alpha > 0$ and $n_\alpha > 0$ such that*

$$\Pr[R \textit{ is } \alpha\textit{-good }] > 0.$$

Proof. Let BAD denote the event that R is not α-good. Let $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n$ be the rows of R and $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_n$ be the columns of R. For any subset $S \subseteq \{1, 2, \ldots, n\}$ with $1 \leq \#S \leq \alpha n$, we define E_S, D_S, A_S, B_S as the events $w(\bigoplus_{i \in S} \mathbf{r}_i) < \alpha n$, $w(\bigoplus_{i \in S} \mathbf{r}_i) > (1 - \alpha)n$, $w(\bigoplus_{i \in S} \mathbf{c}_i) < \alpha n$, $w(\bigoplus_{i \in S} \mathbf{c}_i) > (1 - \alpha)n$ respectively. Then BAD can be written as follows

$$\mathrm{BAD} = \bigcup_{\mathrm{S} \subset [\mathrm{n}], 1 \leq \#\mathrm{S} \leq \alpha \mathrm{n}} \mathrm{A_S} \cup \mathrm{B_S} \cup \mathrm{D_S} \cup \mathrm{E_S}. \tag{7}$$

We analyze A_S for a fixed S. Let $\bigoplus_{i \in S} \mathbf{c}_i = (x_1, x_2, \ldots, x_n)^T$. Since R_{ij} $1 \leq i, j \leq n$ are all independent random variables taking values in $\mathbb{F}_2$, $x_1, x_2, \ldots, x_n$ are n independent uniformly distributed random variables taking values in $\mathbb{F}_2$. We will use Chernoff bounds as given in Theorem 5.1 to analyze the random variable $\#\{i \mid x_i = 1, 1 \leq i \leq n\}$. Let $X = \sum_{i=1}^n x_i$. Then $\mathbf{E}[X] = n/2$. Applying Theorem 5.1 we get

$$\Pr[A_S] = \Pr[X < \alpha n] \leq e^{-\frac{n(1-2\alpha)^2}{4}}.$$

Notice that under $\mathbb{F}_2$ addition $1 + x_1, 1 + x_2, \ldots, 1 + x_n$ are also n independent uniformly distributed random variables taking values in $\mathbb{F}_2$. Thus, by Chernoff bounds we again obtain $\Pr[B_S] \leq e^{-\frac{n(1-2\alpha)^2}{4}}$. Likewise, $\Pr[E_S]$ and $\Pr[D_S]$ are also bounded above by $e^{-\frac{n(1-2\alpha)^2}{4}}$. Putting these together with the definition of BAD in Equation (7) we get

$$\Pr[\mathrm{BAD}] \leq 4\mathrm{e}^{-\frac{\mathrm{n}(1-2\alpha)^2}{4}} \cdot \sum_{\mathrm{i}=1}^{\lfloor \alpha \mathrm{n} \rfloor} \binom{\mathrm{n}}{\mathrm{i}} \leq 4\mathrm{e}^{-\frac{\mathrm{n}(1-2\alpha)^2}{4}} 2^{\mathrm{nH}(\alpha)}$$

where $H(\alpha) = -\alpha(\log \alpha) - (1-\alpha)\log(1-\alpha)$. To ensure that $\Pr[\text{BAD}] < 1$, it suffices to pick $\alpha < 1/4$ such that $H(\alpha) < (\log e)3/8 - 2/n$, which can be done by choosing n larger than some constant n_α and $\alpha > 0$ sufficiently small. ■

From Theorem 5.3, Lemma 5.4, and Remark 3.6 we can immediately deduce the following.

Corollary 5.5 *There are constants $\alpha > 0$ and $n_\alpha > 0$ such that for each $n > n_\alpha$ there is a $[[n, 1, \lfloor \alpha n \rfloor]]_2$ pure quantum stabilizer code. Furthermore, for any β such that $0 < \beta < \alpha$, and $n > n_\alpha$ there is a $[[\lfloor (1-\beta)n \rfloor, \lfloor \beta n \rfloor, \lfloor (\alpha - \beta)n \rfloor]]_2$ pure quantum stabilizer code.*

Remark 5.6 *The above existence argument can be easily extended to stabilizer codes over any finite field. More precisely, for $\mathbb{F}_q$ there are constants $\alpha > 0$ and $n_\alpha > 0$ such that for each $n > n_\alpha$ there is a $[[n, 1, \lfloor \alpha n \rfloor]]_q$ pure quantum stabilizer code. Also, given a β such that $0 < \beta < \alpha$, and $n > n_\alpha$ there is a $[[\lfloor (1-\beta)n \rfloor, \lfloor \beta n \rfloor, \lfloor (\alpha - \beta)n \rfloor]]_q$ pure quantum code.*

Acknowledgment We thank Piyush P Kurur for his help with the computer search for the codes given in Section 4.

References

[1] Alexei Ashikhmin, Emanuel Knill, *Nonbinary quantum stabilizer codes,* IEEE Transactions on Information Theory, vol. 47, No. 7, 3065-3072, 2001.

[2] A. R. Calderbank, Eric M. Rains, Peter W. Shor and N. J. A. Sloane, *Quantum error correction via codes over GF(4),* IEEE Trans. Inform. Theory, Vol. 44 (1998), pp. 1369-1387.

[3] D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, S. S. Somaroo, *Experimental quantum error correction,* Phys.Rev.Lett. 81 (1998) 2152-2155.

[4] D. Gottesman, *A class of quantum error-correcting codes saturating the quantum Hamming bound,* Phys. Rev. A 54, 1862-1868 (1996). Also quant-ph/9604038.

[5] Emanuel Knill, Raymond Laflamme, *A theory of quantum error-correcting codes,* Phys.Rev.Lett. 84 (2000) 2525-2528.

[6] Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, Wojciech Hubert Zurek, *Perfect quantum error correction code,* Physical Review Letters, 98, 77, 1996.

[7] J. H. van Lint, Introduction to Coding Theory, *Springer Verlag,* 3rd edition, 1998.

[8] F. J. Macwilliams and N. J. A. Sloane, Theory of Error-Correcting Codes, *North Holland,* Amsterdam, 1978.

[9] R. Motwani and P. Raghavan, Randomized Algorithms, *Cambridge University Press,* 1995.

[10] Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and quantum Information, *Cambridge,* 1999.

[11] K. R. Parthasarathy, *Lectures on Quantum Computation and Quantum Error-Correcting Codes*, Institute of Mathematical Sciences, Chennai.

[12] E. M. Rains, *Nonbinary quantum codes,* IEEE Transactions on Information Theory, vol. 45, no. 6, pp. 1827-1832, 1999.

[13] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, *A nonadditive quantum code,* Phys.Rev.Lett. 79 (1997) 953-954.

The encoding circuit

We describe the encoding circuit for the stabilizer code with orthonormal basis defined by Equation 6 in the figures below. The elements that we use to build our encoding circuit are the Hadamard gate, the C-NOT gate and the Z gate. We first describe these gates. Then we give the four main components B, $H^{\otimes^n}$, D, and E and finally, the complete encoding circuit in Figure 8.

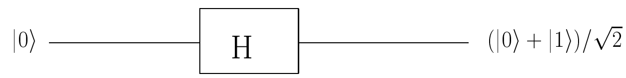

Figure 1: *The Hadamard gate.*

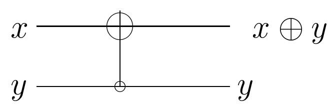

Figure 2: *The controlled NOT gate.*

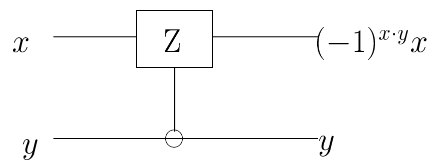

Figure 3: *The controlled Z gate.*

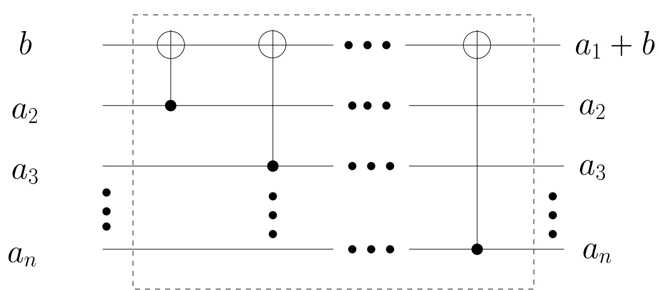

Figure 4: *B: computing* $\mathbf{a} + b\mathbf{e}_1$.

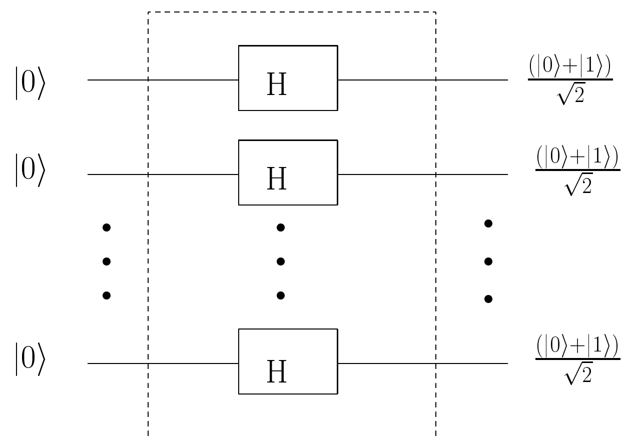

Figure 5: $H^{\otimes^{n-1}}$.

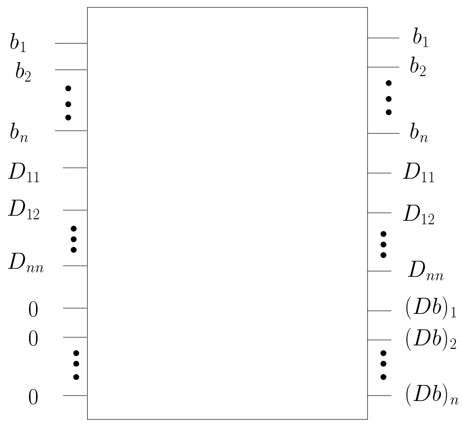

Figure 6: *The linear map D.*

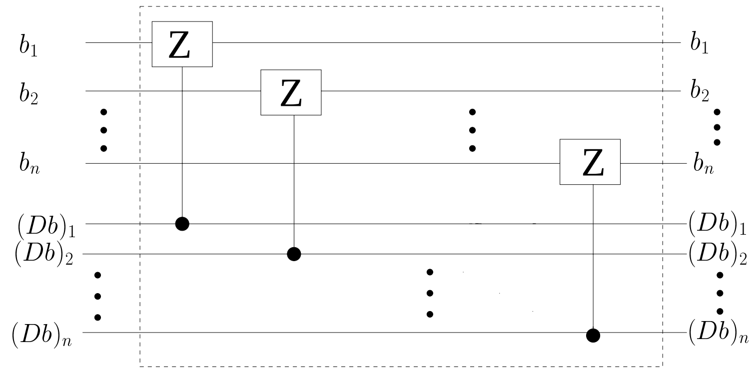

Figure 7: *Component E.*

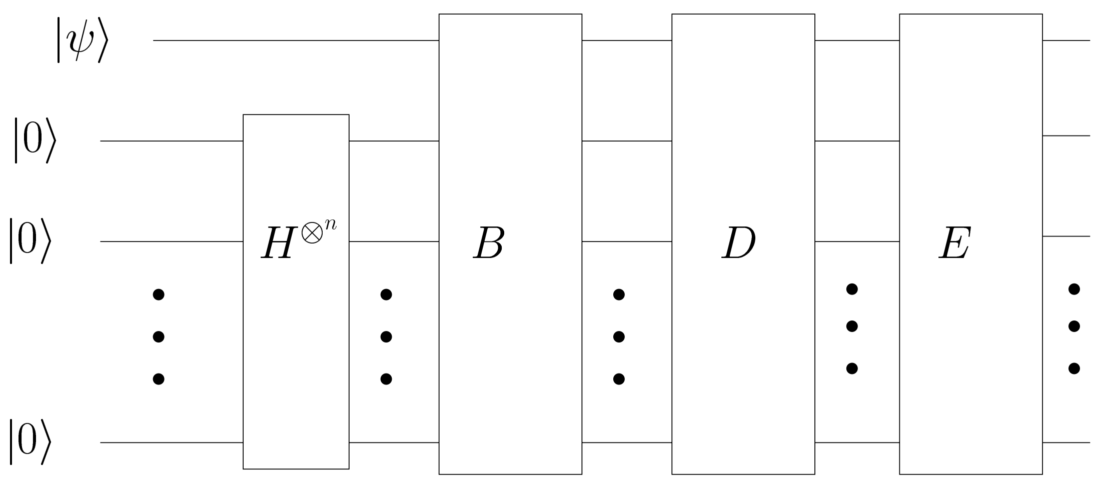

Figure 8: *The encoding circuit.*